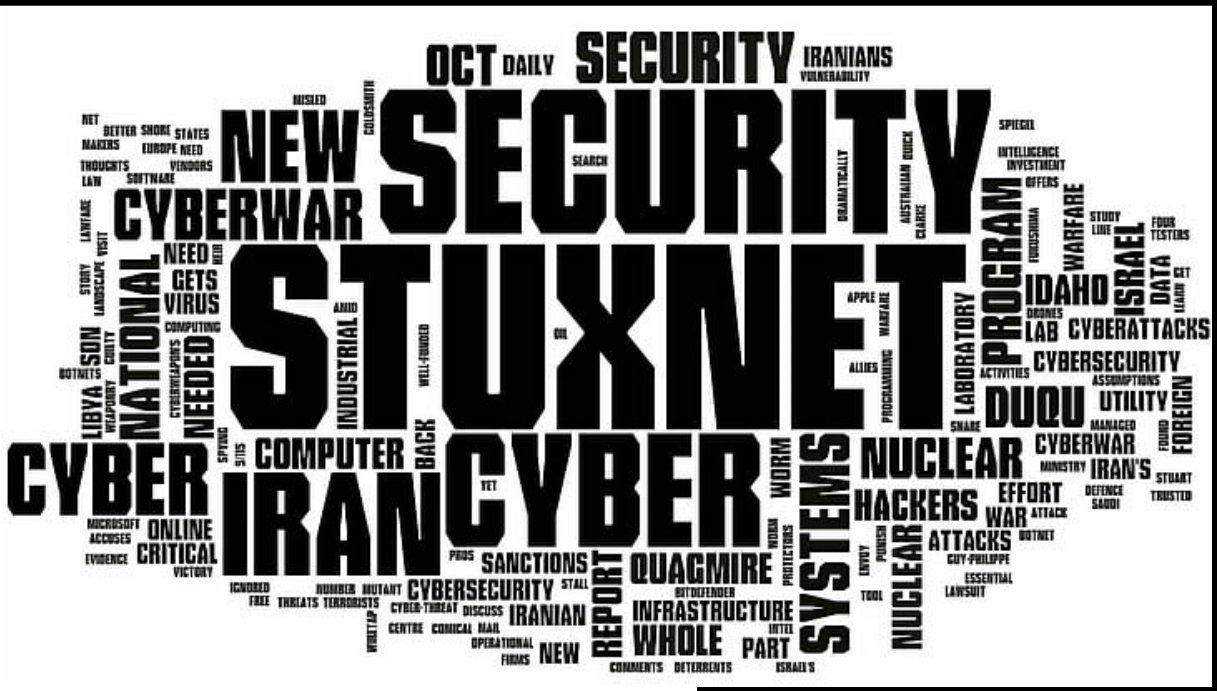
Les cyber-attaques : nouvelle arme étatique, au service du bouleversement du jeu militaire international



Sara Faria Teixeira

Association Werra

Mai 2021

Après un Bachelor en Relations Internationales, **Sara Faria Teixeira** s'oriente en Master vers les domaines de l'Intelligence Stratégique et Économique au sein de l'Institut Libre des Relations Internationales (ILERI). Passionnée par le cyber-renseignement et la géopolitique contemporaine, elle se spécialise dans l'apport des nouvelles technologies de l'information et de la communication dans la géopolitique mondiale.

INTRODUCTION

Dès la création de l'ancêtre d'internet, Arpanet en 1969, l'outil informatique a toujours été utilisé comme support pour la guerre dite « traditionnelle ». Véritable multiplicateur de puissance, la numérisation du champ de bataille a été observée dès la première guerre du Golfe de 1990 à 1991, bien que la première mention du terme « cyber guerrier » se retrouve dans le *Air and Space Power Journa*l de l'année 1996.

Dès lors, les théâtres des conflits accueillent un nouveau cadre d'affrontement et d'expression dans lequel agissent acteurs étatiques et non étatiques sur le même plan : le cyberespace. La particularité de ce nouveau champ de bataille est l'absence de visibilité et de transparence, la difficulté de traçabilité des attaques faisant que l'impunité des incriminé.e.s est courante. Cette absence de hiérarchie nous laisse nous interroger sur l'évaluation de la force, qui dans le cyberespace ne se mesure plus en nombre de divisions blindées ou territoires. Sorte d'asymétrie des combats, internet offre des opportunités d'agréger des individus par-delà les frontières ce qui a pour but d'influencer les États, des opinions publiques, et ainsi permet la diffusion plus rapide et conséquente des idéologies.

Pour définir ce qu'est la cyberguerre, nous pouvons prendre la définition de Michael Gervais dans son article « *Cyber Attacks and the Laws of War* »[1]. Indiquée comme terme générique, la *« cyberguerre regroupe toutes sortes d'actions dans le cyberespace permettant à un groupe étatique ou non étatique, ayant des objectifs définis et une(des) cible(s) bien défini(s), de s'organiser de manière coordonnée passant par la cyberattaque pouvant endommager les systèmes à la cyber-exploitation afin d'obtenir, sans le consentement des victimes, des informations classées confidentielles ».*

Cette notion a été développée à partir du constat observé selon lequel: la dépendance accrue de nos sociétés, gouvernements à l'égard des systèmes informatiques où ce n'est pas nécessairement celui.celle qui a la plus lourde artillerie qui remporte le combat mais celui.celle qui se montrera plus malin que ses pairs. Bien que cette notion connaisse quelques réticences sur son existence[2], les États s'y préparent et les cyberattaques sont de plus en plus courantes dans le monde cybernétique militaire.

[1] Michael Gervais, "Cyber Attacks and the Laws of War", *Yale University - Law School*, 6 octobre 2011, [en ligne], 9 mai 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1939615
[2] Cf : Thomas Rid, *Cyber War Will not take place,* New York, Oxford University Press, 2013, 218 pages

Dans cette nouvelle cohue internationale, on observe donc l'apparition de nouveaux acteurs étatiques et non-étatiques offrant à l'État un champ de possibilité vaste, dans la constitution de sa cyber force. Trois types de recrutement peuvent alors s'opérer : la construction de sa propre force cyber ou d'une espèce de force volontaire, constituée de réserves et enfin l'emploi d'une sous-traitance militaire à travers l'achat de services venant de cyber-mercenaires indépendants ou d'une entreprise privée particulière.

Dans cette réflexion, je vous propose de nous concentrer sur ce dernier cas de figure, et d'oublier notre vision européenne et américano-centrée pour se concentrer sur les actions venant de pays d'Asie, mais aussi du Moyen Orient avec notamment Israël et l'Iran qui depuis des années, se livrent une cyberguerre continue. Ce point est intéressant lorsque l'on sait que les premières mentions d'une cyberguerre se retrouvent dans les actions des hackers serbes en 1999 suite au bombardement de l'OTAN ou encore dans la vague de cyberattaque de la Russie envers l'Estonie en 2007. Depuis, la Russie comme d'autres, ne cessent de développer leurs techniques offensives, rivalisant ainsi avec d'autres grandes puissances qu'ils n'hésitent pas à déstabiliser les règles du jeu cyber, différentes de la guerre « physique ».

Ainsi, nous pouvons nous poser les questions suivantes :

Comment les cyber guerriers des pays d'Asie et du Moyen Orient dominent la cyberguerre étatique ? Leurs actions peuvent-elles être considérées comme des actes de guerre ? Quelles conséquences rencontreront ces États ainsi que ces mercenaires dans la guerre d'aujourd'hui ?

Pour répondre à ces questions, nous allons voir dans un premier temps que l'absence d'un droit contraignant et partagé par tous permet à ces entités d'exercer leurs activités et du développement de facto de leur compétences. Dans un second temps, nous allons observer comment ces actions se traduisent sur la scène dite « physique » et quelles en sont les conséquences pour la paix internationale.

Un contexte propice au développement de la cyber guerre

Un jeu international, des règles différentes selon les États

Pour commencer, plusieurs données sont à prendre en compte. Sans rentrer directement dans le jus ad bellum – droit à la guerre – il n'y a pas de consensus juridique contraignant universel sur la régulation des activités du cyberespace. Il y a bien entendu eu des initiatives comme la Convention de Budapest sur la cybercriminalité de 2006 ou encore la déclaration d'indépendance du cyberespace de 1996. Pourtant, alors que dans le premier cas, la convention témoigne d'une prise de conscience de l'impact des cyberattaques sur la vie des individus, elle n'a pas été assez ratifiée pour pouvoir jouir d'un pouvoir contraignant. La déclaration d'indépendance ne pouvant pas être appliquée car aucun Etat ne l'a signée et donc elle ne relève pas du droit international.

Aujourd'hui, il n'y a donc pas d'accord ou de traité qui puisse dicter aux États la conduite à adopter lors de ces actions dans le cyberespace[3]. Pour aller encore plus loin, il n'y a pas d'actions collectives internationales permettant aux États de pouvoir s'organiser surune base commune.

Cela vient également du fait qu'au niveau national, chaque État définit ses propres termes d'une cyberattaque et de ses limites légales. Par exemple le rapport aux données personnelles n'est pas le même en fonction des régions du globe, ce qui permet notamment à la Chine de s'infiltrer sur le marché européen malgré le Règlement général de la protection des données (RGPD).

Pour autant, cela ne veut pas dire que les victimes de cyberattaques n'ont pas de bases légales sur lesquelles s'appuyer. Surtout lorsque ce domaine touche à la guerre !

De ce côté-ci, plusieurs dispositions venant limiter un cadre dans lequel s'exprime la légalité de la guerre sont déjà mises en place. Nous pouvons citer l'article 2§4 de la Charte des Nations-Unies[4] qui limite le « recours à la force » d'un État sur un de ses pairs. Cependant, là encore, il n'y a pas de consensus sur l'interprétation de la « force » en droit international, cette notion étant mise en perspective avec la Convention de Vienne sur le droit des Traités de 1969 et plus

[3] Camille Rabussier, *L'application du droit international dans le cyberespace*, Université Paris II Panthéon Assas, 2019, [en ligne], 7 mai 2021, disponible sur : http://idc.u-paris2.fr/sites/default/files/memoires/Mémoire%20Camille%20Rabussier%20Application%20du%20droit%20international%20dans%20le%20cyberespace.pdf

[4] Charte des nations Unies de 1945- Article II paragraphe IV : https://www.un.org/fr/sections/un-charter/chapter-i/index.html

particulièrement son article 31[5] qui offre une pluralité d'interprétation pour ce cas-ci. De plus, dans le cas d'un conflit guerrier, il faut démontrer que la cyberattaque a atteint le seuil de l'attaque armée pour prévoir des représailles prévues à l'article 51 de la Charte de l'ONU.

Ainsi, les règles et les limites qui régissent le droit international, sous toutes leurs formes, restent floues, ce qui donne aux États une marge de manœuvre assez imposante. De même, la difficulté de traçabilité des cyberattaques est un facteur attrayant. Il semble donc, que pour l'instant, le développement rapide des nouvelles technologies comparés à la mise en place lente d'un appareil juridique international et contraignant constitue un terrain favorable aux actions cyber des États sur la scène internationale.

Une sous-traitance indispensable d'État à cyber-mercenaires

Le nerf de la guerre, c'est l'information. Or avec l'arrivée d'internet, et la dépendance croissante de nos sociétés envers l'outil informatique, le monopole de l'information n'est plus un privilège étatique. À ce fait s'ajoute que le cyberespace donne à la notion de la guerre une toute nouvelle dimension qui contraint les États à développer leurs compétences, pour ainsi tenter de reprendre la main sur le contrôle du cyberespace. Dans cette optique, il n'est plus rare de voir aujourd'hui une coopération entre les États et des groupes privés, des mercenaires, des cyber-guerriers. Cette notion reste tout de même assez large et peut regrouper toutes sortes de spécialistes : des hackers, des spécialistes en renseignement ou encore des acteurs experts en technique de défense offensive.

Cette coopération, nous la retrouvons chez toutes les puissances technologiques aujourd'hui. On les retrouve bien évidemment en Russie, avec le groupe de hackers *Sandworm et Fancy Bears* ayant des présumés liens avec son État d'origine, mais aussi en Syrie avec les cyberpirates de l'armée électronique syrienne ayant des liens très étroits avec le régime de Bashar al-Assad. Mais aussi en Corée du Nord où l'un de ces groupes serait à l'origine de l'une des plus grandes cyberattaques qu'ont connu les systèmes informatiques du monde entier : Wannacry 2017. Ayant des versions circulant encore dans le cyberespace, Wannacry est un rançongiciel – programme malveillant chiffrant les données de ses victimes pour leur extorquer de l'argent – infectant les systèmes d'exploitation de Windows 7 où on estime que 98% des ordinateurs avec ce système ont été touchés sur 300000 victimes recensées. Pour en savoir plus

[5]Convention de Vienne sur le droit des Traité de 1969 – Article 31 : https://legal.un.org/ilc/texts/instruments/french/conventions/1_1_1969.pdf

sur le sujet, il a par ailleurs été largement développé dans la série d'articles cyberguerre « Numérama » de 2018 qui donne une approche globale et technique de ce virus ayant paralysé des millions de victimes dans le monde entier[6].

Ces groupes représentent donc un avantage stratégique non-négligeable pour les États qui les emploient. Par l'intermédiaire d'internet, seule une connexion et beaucoup d'imagination suffisent pour pouvoir nuire à un pouvoir étatique. Des stratégies indirectes qui peuvent affaiblir tout un secteur économique d'un pays, servent les intérêts d'un autre et lui confèrent des avantages concurrentiels qu'il n'aurait pas pu avoir, s'il n'avait pas eu recours à ce genre de pratique. En temps de conflit comme de paix, les actions de cyber espionnage et d'ingérence politique ne sont pas effacées pour autant, se multipliant même avec la crise du Covid-19. La nécessité donc de s'armer de professionnel.le.s au-delà de toutes morales et de toutes lois devient un enjeu primordial pour les puissances technologiques tant dans leur stratégie défensive qu'offensive. Les Etats sont ainsi les plus grands pirates avec 87% du cyber espionnage mondial réalisé par des États en 2013[7], un point que nous allons développer dans cette seconde partie.

Pérennisation d'une puissance technologique et stratégie de déstabilisation

Le cyber-espionnage : déstabilisateur de la paix mondiale

Le cyber espionnage est devenu l'une des activités principales du cyber militaire des armées russes, chinoises, israéliennes ou encore nord-coréennes. Elle a pour but de s'infiltrer discrètement dans les systèmes informatiques de particuliers ou bien d'organisations pour pouvoir avoir accéder à toutes sortes de données pour les récupérer et les exploiter. Ces actions peuvent se regrouper en plusieurs stratégies : le sabotage, la contre-propagande, l'exploitation des ressources ou encore le (contre) terrorisme. Énormément développé depuis le début de la

[6] Vic Castro, « WannaCry, un an après : aux origines d'une des plus grandes cyberattaques de tous les temps », Cyberguerre, 2018, [en ligne], 6 mai 2021. Disponible sur : https://cyberguerre.numerama.com/170-wannacry-un-an-apres-aux-origines-dune-des-plus-grandes-cyberattaques-de-tous-les-temps.html

[7] « Cyberespionnage, les États sont les plus grand pirates » , La Tribune, avril 2014, [en ligne], 6 mai 2021. Disponible sur : https://www.latribune.fr/technos-medias/20140422trib000826288/le-cyber-espionnage-augmente-surtout-en-europe-de-l-est.html

pandémie, le cyber espionnage n'est pas nouveau, les premières traces connues du grand public remontant en 2007 avec la cyberguerre entre la Russie et l'Estonie.

Très récemment a eu lieu l'affaire « *Solarwinds* », l'opération de cyber espionnage la plus sophistiquée de ces dernières années. Pour les autres, voici un petit récapitulatif : en décembre 2020, une entreprise spécialisée dans la chasse aux hackers étatiques et proche des services américains de renseignement, *FireEye*, a dévoilé publiquement la mise en place de nombreuses actions sophistiquées de cyber espionnage envers l'entreprise Solarwinds, une société américaine proposant à de grandes instances américaines ses services spécialisés notamment dans la conception de logiciels de gestion informatique[8]. Passant par une backdoor[9] d'un des logiciels, Orion, les hackers définit comme hautement qualifiés ont implanté un malware pour s'introduire dans le système des entreprises américaines. La médiatisation de cette affaire a été immédiate pour plusieurs raisons.

Tout d'abord, l'extrême sophistication du malware, baptisé Sunburst, est à prendre en compte. Exploitant les services de ses victimes depuis le printemps 2020, il permettait à ses créateurs d'entamer des manœuvres d'espionnage contre des organisations gouvernementales et leurs collaborateurs. De plus, pas moins d'une vingtaine de grandes instances étatiques sur les 300 000 clients de Solarwinds a été répertoriée comme victimes de l'attaque selon Reuters et une étude du New-York Times. Parmi elles, de grandes instances américaines comme le Trésor américain, le *Department of Homeland Security* qui, ironie du sort, a pour mission de protéger les citoyens face aux cyberattaques du monde entier, l'Administration nationale des télécommunications et de l'information mais aussi Microsoft et FireEye, déclarant avoir été eux-mêmes victimes de cette faille informatique. Solarwinds, diffusant sans le savoir, le malware à 18 000 autres entités[10] a permis pendant quelques mois aux hackers d'accéder à des e-mails confidentiels et aux systèmes d'information des victimes.

Si un bon nombre de groupes étatiques ont été pointé du doigt, les États -Unis, après quelques mois d'hésitation, ont décidé d'accuser la Russie de cyber espionnage. A l'avenir, des sanctions

[8] "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor", FireEye, 2020 [en ligne], 6 mai 2021. Disponible sur : https://www.fireeye.fr/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[9] Selon l'Agence Nationale de la Sécurité des Systèmes d'Information, une backdoor aussi appelé porte dérobée est un « accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive »

[10] François Manens, « Sunburst : le gouvernement américain n'est qu'une victime parmi 18 000 autres », Cyberguerre, 2020, [en ligne], 14 mars 2021. Disponible sur : https://cyberguerre.numerama.com/9409-sunburst-le-gouvernement-americain-nest-quune-victime-parmi-18-000-autres.html

sont prévues avec l'expulsion de 10 diplomates russes du territoire américain et des nouvelles mesures du Trésor américain à l'encontre de 6 entreprises russes soupçonnées d'avoir contribuer à ces actions. Cette affaire prenant vite une tournure de crise diplomatique, mêlant l'OTAN qui a appelé son ennemi historique à « immédiatement cesser ses comportements déstabilisateurs, et à respecter ses obligations internationales »[11].

Ainsi, réel outil de perturbation de la paix internationale, le cyber espionnage s'est fortement développé et n'est plus un cas aujourd'hui. Selon Franck DeCloquement, elles ont toutes un point commun : l'apprentissage et la mise en pratique d'un art de l'imagination et de la supercherie employés par des acteurs malveillants pour parvenir à leurs fins en plaçant l'aspect humain au centre des opérations12. En effet, ayant pourtant de nombreux points faibles, l'aspect humain peut pallier la course aux nouvelles technologies d'aujourd'hui qui possède un coût énorme pour les États concurrents. Le champ d'application du cyber espionnage ne semble pas avoir de limite, échappant souvent aux acteurs qui l'utilisent. Ainsi les soupçons de cyber espionnage sont souvent source d'accusations où la vérité n'est pas essentielle, le plus convaincant l'emportant sur tout le reste.

Son application et ses conséquences sont souvent prises en compte, ils influencent inévitablement les relations internationales par leurs caractères ambiguës et leur manque de transparence, idéal pour des actions secrètes. Véritable outil de contestation de la paix occidentale mise en place depuis la Chartre de L'ONU, les conflits n'opposent pas toujours les puissances euro-américaines aux autres. Elle est aussi l'expression des conflits entre les puissances émergentes, comme en novembre 2020, où le Brésil a ouvertement accusé sur les réseaux sociaux la Chine, de pratiquer du cyber espionnage grâce au déploiement de la 5G dans le monde entier. Cet aveu fait échos à la décision du pays sud-américain de s'allier à la politique de la superpuissance américaine incarnée par Donald Trump à cette époque. Ainsi ironiquement, le cyber espionnage est aussi un bon moyen de dresser un panorama du jeu des alliances se profilant entre les différents pays sur la scène internationale.

---

[11] *Déclaration du Conseil de l'Atlantique Nord suite à l'annonce par les États-Unis de mesures concernant la Russie*, North Atlantic Treaty Organization, Communiqué de presse, avril 2021, [en ligne], 01 mars 2021. Disponible sur : https://www.nato.int/cps/en/natohq/news_183168.htm?selectedLocale=fr

[12]Franck DeCloquement, « ESPIONNAGE, ATTAQUES SUBVERSIVES ET CYBER SÉCURITÉ : DE L'IMPACT DES ACTIONS DE « SOCIAL ENGINEERING » ET DES VULNÉRABILITÉS HUMAINES SUR LA SÉCURITÉ GLOBALE DES ENTREPRISES »,Sécurité et Stratégie, 2016 [en ligne], 14 mars 2021. Disponible sur : https://www-cairn-info.bdd.monbureauvirtuel.net/revue-securite-et-strategie-2016-2-page-21.htm

Ce phénomène est donc beaucoup utilisé par les pays émergents, comme par exemple l'Opération Cleaver, riposte iranienne de 2014 suite à l'attaque de Stuxnet en 201413. Comme vu en introduction, le cyberespace n'est plus l'apanage de la société civil et les services de renseignement utilisent désormais les nouvelles technologies pour effectuer leurs actions. Son champ d'application évolue et les pays se dotent de plus en plus de cellules dédiées à cet effet. C'est le cas d'Israël avec la fameuse unité 8200 ou de l'unité Hatzav chargée du renseignement militaire sur sources ouvertes (OSINT)14 et la *National Cybernetic Taskforce*, créée en 2011 chargée du contre-espionnage industrielle et du cyber terrorisme.

Expression de la cyber-guerre par la guerre d'information : ingérence et actes politiques

Depuis les traités de Westphalie de 1648, le respect de la souveraineté des États est primordial dans la conduite des relations internationales. Son application relève d'une autre règle, considérée comme coutumière: le droit de non-ingérence. Bien qu'ambigüe, il désigne le fait qu'un État est souverain sur son territoire, et qu'il est donc interdit pour un État extérieur d'interférer dans les affaires intérieures de l'un de ses pairs.

L'obligation de s'y tenir est formulé notamment à l'article 2§7 de la Charte des Nations Unies, entrée en vigueur en 1945 : *« Aucune disposition de la présente Charte n'autorise les Nations Unies à intervenir dans des affaires qui relèvent essentiellement de la compétence nationale*

d'un État ni n'oblige les Membres à soumettre des affaires de ce genre à une procédure de règlement aux termes de la présente Charte »[15].

Bien qu'en principe, aucun État ne doit, transgresser ces textes de lois, l'application de ces derniers semblent moins clairs qu'il n'y parait. Comme souligné dans la première partie de cette réflexion, lorsqu'une règle de droit est établie, les États trouveront toujours un moyen de la contourner pour pouvoir servir leurs intérêts. L'exercice de la guerre dans le cyberespace ne fait pas exception !

[13]Reynald Fléchaux, « Opération Cleaver : la riposte des Iraniens à Stuxnet ? », Silicon, 4 décembre 2014, [en ligne], 01 mars 2021. Disponible sur : https://www.silicon.fr/operation-cleaver-la-riposte-des-iraniens-stuxnet-103309.html#

[14]Nicolas Ténèze, « Israël : la « supériorité numérique » du Moyen-Orient », *Revue Défense Nationale*, 2015 (n°784), en ligne], 28 mars 2021. Disponible sur : https://www-cairn-info.bdd.monbureauvirtuel.net/revue-defense-nationale-2015-9-page-58.htm

[15] Charte des nations Unies de 1945- Article II paragraphe VII : https://www.un.org/fr/sections/un-charter/chapter-i/index.html

Lorsqu'un(e) étudiant(e), expert(e) en relations internationales pense à « ingérence d'un État » dans les affaires d'un autre, il/elle pense souvent au rôle de la Russie dans la campagne présidentielle des États-Unis de 2016. Bien que ce ne soit pas considéré comme un acte de guerre, cela nous montre bien comment l'outil informatique est utilisé à des fins d'ingérence. Pourtant, son application relève bien d'une composante de la cyberguerre : la guerre d'information. En effet, sa maitrise a toujours été un enjeu essentiel pour les États utilisant les systèmes d'informatiques pour effectuer de la désinformation ou de la propagande[16].

De manière plus générale, les cyberattaques sont souvent un moyen d'expression de leur mécontentement par rapport à certaines mesures prises pour un pays donné. Par exemple, en 2007, lors de la campagne de cyberattaque de grande ampleur menée en Estonie par la Russie, le pays a voulu montrer son mécontentement suite au démontage d'un monument à la gloire de l'Armée rouge à Tallinn, en s'attaquant aux réseaux des gouvernements des banques puis des partis politiques afin de décrédibiliser les dirigeants du pays.

Une autre information importante, selon Michael Gervais[17], le vol des informations confidentielles à un gouvernement en s'introduisant dans leurs systèmes informatiques peut être considéré aussi comme une ingérence diplomatique. Pour arriver à ces fins, plusieurs outils sont utilisés, la seule condition est d'avoir une connexion internet. Le lancement de malware paralysant les systèmes informatiques de la cible, l'introduction de *botnet* - diminutif de robot et de network, sont un ensemble d'appareils électroniques rassemblés en réseaux et n'obéissant qu'au propriétaire du malware qui les infecte – pour attaquer les DDOS sont courants. Ils permettent ainsi aux hackers de pouvoir contrôler l'information et de l'utiliser à leur avantage.

Le cas Stuxnet

Bien que le virus Stuxnet ait été découvert en 2010, sa mise en application remonte à 2005. Malware complexe ayant pour but de saboter le fonctionnement des systèmes des centrifuges iraniennes, cette attaque reste inédite car pour la première fois, l'opinion publique découvre qu'une cyberattaque peut être quelque chose de complexe, préparée à un tel niveau qu'elle relève de l'espionnage industrielle. En effet, le virus exploite des zeroday (0-day) : c'est-à-dire une faille non connue par son programmeur lors de sa création et sa mise en marché mais qui reste efficace. Ce n'est pas moins de 4 zeroday exploités par les systèmes Microsoft utilisés

[16]Michel Baud, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique Étrangère*, 2012, en ligne], 18 mars 2021. Disponible sur : https://www.cairn.info/revue-politique-etrangere-2012-2-page-305.htm#re6no6

[17] Michael Gervais, "Cyber Attacks and the Laws of War", *Yale University - Law School*, 6 octobre 2011, [en ligne], 9 mai 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1939615

par la centrale nucléaire de Natanz en Iran pour ralentir le programme en place. Ce dernier a pour but de développer les travaux sur l'enrichissement de l'uranium, fortement remis en cause par les communautés internationales, voyant le programme comme une déstabilisation de la sécurité régionale.

Selon les analyses du journal cnet[18], le virus a été mis en place à l'aide d'une simple clé USB, implantant un rootkit[19] qui a non seulement attaqué les automates programmables contrôlant les centrifugeuses mais qui s'est aussi répandu dans le cyberespace mondial.

Tout cela ne pouvait que s'arrêter là, et pourtant ! En 2013, Edward Snowden, ancien informaticien de la NSA dévoile que derrière Stuxnet se cachaient les États-Unis et Israël. Une nouvelle qui sera plus tard confirmée par une enquête du New York Times réaffirmant le rôle des deux pays dans l'affaire. Le journal déclare également l'importance de ce programme, étant intégré à une initiative plus large de contrôle des essais nucléaires de l'Iran, une volonté du gouvernement de George W. Bush qui se serait transmise aux 44ème président des États-Unis, Barack Obama, acceptant de continuer la manœuvre, malgré les suspicions déjà existantes envers la superpuissance.

[18] Daniel Terdiman, "Stuxnet delivered to Iranian nuclear plant on thumb drive" *Cnet*, 12 avril 2012, , [en ligne], 8 mai 2021. Disponible sur :https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

[19] Définition issue du groupe Kaspersky, je cite : « un rootkit est un terme anglais qui désigne un type de malware conçu pour infecter un PC et qui permet au pirate d'installer une série d'outils qui lui permettent d'accéder à distance à un ordinateur ». Dispobible sur : https://www.kaspersky.fr/blog/quest-ce-quun-rootkit/750/

CONCLUSION

Pour conclure, nous pouvons dire que l'absence d'un corpus de lois contraignant les actions des États sur la scène cybernétique a permis aux puissances asiatiques et du Moyen Orient de développer leurs compétences militaro-technologiques. Véritable paradis digitaux[20], cela conduit à un changement de la doctrine de la guerre, où aucune notion coercitive de dissuasion n'est prévue ; malgré le caractère dangereux et brutal qu'engendrent les cyberattaques sur nos systèmes industriels, politiques, économiques. Une réelle prise de conscience a été établie dès les prémisses de cette cyberguerre de grande envergure comme lors de *Wannacry* ou encore *Meow*, sur la nécessité de se doter d'un appareil offensif dans un monde où la plupart de nos infrastructures de défense et sécurité reposent sur l'outil informatique.

Plus que jamais, la guerre pour l'information est devenue la principale préoccupation des États. Qui contrôle l'information et ses moyens de communication, contrôle le monde[21]. Dans cette optique, on observe une multiplicité des attaques à des fins d'espionnage ou encore de sabotage venant des pays du Moyen Orient ou d'Eurasie, comme l'une des plus grandes cyberattaque de notre ère, *Wannacry* qui aurait été perpétuée par un groupe nord-coréen *Lazarus*.

Véritable contestation du système politique, économique, universaliste mis en place depuis 1945, les cyberattaques deviennent de plus en plus sophistiquées, ciblées et impactantes, mettant en lumière une multitude d'acteurs pourtant la plupart du temps difficile à identifier. La guerre moderne se passera donc en partie dans le cyberespace, un cadre où Israël, l'Iran, la Chine ou encore la Russie, se sont construits une réputation de leader dans le monde des cyber-pirates.

[20] Par analogie au paradis fiscal, une notion mise en place dans l'article de Solange Ghernaouti-Hélie, « Menaces, conflits dans le cyberespace et cyberpouvoir », *Sécurité et Stratégie*, 2011, 12 avril 2012, , [en ligne], 8 mai 2021. Disponible sur : https://www.cairn.info/revue-securite-et-strategie-2011-3-page-61.htm#re6no6

[21] Comme le dirait Glen Otis, général américain : *« Le combattant qui l'emporte est celui qui gagne la campagne de l'information. Nous en avons fait la démonstration au monde : l'information est la clef de la guerre moderne – stratégiquement, opérationnellement, tactiquement et techniquement.* »